UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,860	07/25/2001	Michael L. Wenocur	A-70558/RMA	6189

7590 05/10/2005

FLEHR HOHBACH TEST ALBRITTON & HERBERT, LLP
Suite 3400
Four Embarcadero Center
San Francisco, CA 94111

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/912,860	**Applicant(s)** WENOCUR ET AL.
	Examiner Ronald Baum	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10-20,22* is/are rejected.

7)☒ Claim(s) *9 and 21* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *2/11/02*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-22 are pending for examination.

2. Claims 1-8,10-20,22 are rejected.

3. Claims 9,21 are objected to.

Claim Rejections - 35 USC § 112

4. The term "using *less* software code and network bandwidth ..." in claim 2, is a relative term which renders the claim indefinite. The term "... *less* ..." is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For the purpose of applying art, the phrase encompassing the term will not be considered. Correction is required.

Further, the term "... *widely known*" in claim 15, is a relative term which renders the claim indefinite. The term "... *widely* ..." is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For the purpose of applying art, the phrase encompassing the term will not be considered. Correction is required.

Further, the term "... *widely known* " in claim 16, is a relative term which renders the claim indefinite. The term "... *widely* ..." is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For the purpose of applying art, the phrase encompassing the term will not be considered. Correction is required.

Further, the term "... is difficult to discover ..." in claim 16, is a relative term which renders the claim indefinite. The term "... *difficult* ..." is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For the purpose of applying art, the phrase encompassing the term will not be considered. Correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 17-20,22 are rejected under 35 U.S.C. 102(e) as being anticipated by Montville et al, U.S. Patent 6,356,937 B1.

6. As per claim 17; "A method for secure unidirectional messaging from a sender to a recipient, said method comprising [Montville et al, figures 1-4 and associated descriptions, col. 3,lines 5-col. 4,line 15, col. 5,lines 5-65]:

obtaining, by the sender,

a

public key and

destination address of a message recipient and

the

senders own private signing key and

certificate chain from one or more trusted source [figures 9-14 and associated descriptions, whereas the setup of recipient routing information, at the very least, via the user interface, clearly encompasses the "... obtaining ... key ... address ... certificate ...", as broadly interpreted by the examiner.];

passing, by the sender,

the

extracted public key and

matching destination address and

private signing key and

certificate chain information, and

the

data of an intended message along with

the recipient's public enveloping key and

a random data encryption key and

random padding seed to a cryptographic primitive [figures 1-14 and associated descriptions, whereas the setup of recipient routing information and subsequent processing to setup the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "...passing ... with ...", as broadly interpreted by the examiner.]; and constructing, by the sender,

a secure unidirectional message there from [figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "... constructing ... unidirectional message ...", as broadly interpreted by the examiner.]."

7. Claim 18 ***additionally recites*** the limitation that; "The method of claim 17, further comprising:

sending, by the sender, the constructed secure unidirectional message to the recipient."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "... sending ... unidirectional message ...", as broadly interpreted by the examiner.).

8. Claim 19 ***additionally recites*** the limitation that; "The method of claim 18, further comprising:

receiving the secure unidirectional message by the recipient figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "...receiving ...", as broadly interpreted by the examiner.;

extracting, by the Recipient, the recipient's own private key from a secure source and

decrypting

the public key encryption, and

the data encryption key and

decrypting the data which is digitally signed; and

verifying the signature of the data and the certificate chain of the sender."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "…extracting … decryption … verifying …", as broadly interpreted by the examiner.).

9. Claim 20 ***additionally recites*** the limitation that; "The method of claim 18, wherein said message is an e-mail message."

The teachings of Montville et al are directed towards such limitations (i.e., figures 9-14 and associated descriptions, whereas the setup of recipient routing information, at the very least, via the user interface, clearly encompasses the "… e-mail …", as broadly interpreted by the examiner.).

10. Claim 22 ***additionally recites*** the limitation that; "The method of claim 18, wherein

the trusted source or

storage means comprises

a Compact Certificate as explained earlier, or

chain of Compact Certificates leading to a trusted root public key."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "...certificate ... trusted root public key ...", as broadly interpreted by the examiner.).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-8,10-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Montville et al, U.S. Patent 6,356,937 B1, and further in view of Bellare, M., et al, "VarietyCash: a Multi-purpose Electronic Payment System", 8/31/1998, USENIX Workshop for electronic commerce,

http://www.usenix.com/publications/library/proceedings/ec98/full_papers/bellare/bellare.pdf.

12. As per claim 1; "A computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising

a computer readable storage medium [Montville et al, col. 3,lines 5-col. 4,line 15, col. 5,lines 5-65] and

a computer program mechanism embedded therein, the computer program mechanism, comprising [Montville et al, col. 3,lines 5-col. 4,line 15, col. 5,lines 5-65]:

a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications [Montville et al, figures 1-4 and associated descriptions, col. 3,lines 5-col. 4,line 15, col. 5,lines 5-65], the message communications occurring in a

computer system hardware architecture neutral and

operating system neutral and

network transport protocol neutral manner for secure unidirectional messaging [Montville et al, figures 1-4 and associated descriptions, col. 3,lines 5-col. 6,line 12, whereas the robust and scaleable aspects, in addition to Windows and MAC compatible embodiments clearly, as broadly interpreted by the examiner, encompass the limitations], the program module including instructions for:

A. extracting, by the sender,

an appropriate public key and

matching destination address of a Recipient from a storage means that is trusted and has been verified [figures 9-14 and associated descriptions, whereas the setup of recipient routing information, at the very least, via the user interface, clearly encompasses the "...extracting ... key ... address ...", as broadly interpreted by the examiner.];

B. extracting, by the sender,

the senders own private signing key and

certificate chain from a trusted storage means [figures 9-14 and associated descriptions, whereas the setup of recipient routing information, at the very least, via the user interface, clearly encompasses the "...extracting ... key ... certificate ...", as broadly interpreted by the examiner.];

C. passing, by the sender, that extracted

public key and

matching

destination address and

private signing key and

certificate chain information, and

the data of the message along

with

the Recipient's public enveloping key, and

a fresh random data encryption key and

fresh random OAEP padding seed

to the Signed-Inside-Enveloped-Data cryptographic primitive to construct a secure unidirectional message [figures 1-14 and associated descriptions, whereas the setup of recipient routing information and subsequent processing to setup the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "...passing ... with ...", as broadly interpreted by the examiner.];

D. sending, by the sender, the constructed secure unidirectional message [figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "...sending ...", as broadly interpreted by the examiner.];

E. receiving, by the Recipient, the message [figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "...receiving ...", as broadly interpreted by the examiner.];

F. extracting, by the Recipient, its own private key from a secure storage means and

decrypting the public key encryption [figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "...extracting ... decryption ...", as broadly interpreted by the examiner.];

G. extracting, by the Recipient, the data encryption key, and

decrypting the data which is digitally signed [figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "...extracting ... decryption ...", as broadly interpreted by the examiner.]; and

H. verifying the signature of

the data and

the certificate chain of the Sender [figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon receipt, at the very least, clearly encompasses the "... verifying ... data ... certificate ...", as broadly interpreted by the examiner.];

I. wherein this is done using the same cryptographic primitive that is the same as the cryptographic primitive used with at least a secure session protocol [figures 1-14 and associated descriptions, whereas the email/message transfer and transfer configuration aspects upon subsequent receipt, at the very least, clearly encompasses the "...same cryptographic primitive ...", as broadly interpreted by the examiner.]."

13. Further, as per claim 2, this claim is the method claim for the embodied software claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, as such; "A

hardware architecture neutral and

operating system neutral and

network transport neutral method for secure unidirectional messaging using less software code and network bandwidth than conventional systems, said method comprising:

A. extracting, by the sender,

an appropriate public key and

matching destination address of a Recipient from a storage means that is trusted and has been verified;

B. extracting, by the sender, the sender's own

private signing key and

certificate chain from a trusted storage means;

C. passing, by the sender, that extracted

public key and

matching

destination address and

private signing key and

certificate chain information, and

the data of the message along

with

the Recipient's public enveloping key, and

a fresh random data encryption key and

fresh random OAEP padding seed

to the Signed-Inside-Enveloped-Data cryptographic primitive to construct a secure unidirectional message;

D. sending, by the sender, the constructed secure unidirectional message;

E. receiving, by the Recipient, the message;

F. extracting, by the Recipient, its own private key from a secure storage means and

decrypting the public key encryption;

G. extracting, by the Recipient, the data encryption key, and

decrypting the data which is digitally signed; and

H. verifying the signature of

the data and

the certificate chain of the Sender;

I. wherein this is done using the same cryptographic primitive that is the same as the cryptographic primitive used with at least a secure session protocol."

The teachings of Montville et al suggest the base claim ("... server and a client ... program product comprising ... storage medium ... program mechanism ... to provide message communications, ... hardware architecture neutral and operating system neutral and network transport protocol neutral manner for secure unidirectional messaging, ... extracting, ... public key ... destination address of a Recipient ... senders own private signing key and certificate chain ... passing, ... key ... address ... signing key ... chain information, ... message ... public enveloping key, ... data encryption key and fresh random OAEP padding seed to ...Enveloped-

Data cryptographic primitive to construct … message; … sending, … message; … receiving, … decrypting … the data which is digitally signed; … least a secure session protocol…") limitations (see "As per claim 1 …" paragraph above) *without explicitly teaching* of the use of the "random OAEP padding seed".

Bellare, M., et al, teaches of using a "random OAEP padding seed" in message encrypted protocols.

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Montville et al encrypted E-mail messaging system, with the Bellare, M., et al teachings of the use of RSA OAEP in order to "provide secrecy, … message integrity … [see, Bellare, M., et al, section 2.4, 7th full paragraph]".

Such motivation to combine would clearly encompass the need to allow secure cryptographic parameter (i.e., the seed for such cryptographic functionality) insofar as the whole point of having secure message integrity to prevent "chosen-cyphertext attacks" (i.e., again, Bellare, M., et al, section 2.4, 7th full paragraph).

14. Further, as per claim 3 ***additionally reciting*** the limitation that; "The method in claim 2, wherein said appropriate public key comprises an RSA based public key."

The teachings of Montville et al are directed towards such limitations (i.e., col. 6,lines 51-col. 12,line 42, whereas RSA, clearly encompasses the "…public key … RSA based public key", as broadly interpreted by the examiner.).

15. Further, as per claim 4 ***additionally reciting*** the limitation that; "The method in claim 2, wherein said matching destination address is selected from the set consisting of

an e-mail address and

a URL."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of recipient routing information, at the very least, via the user interface, clearly encompasses the "...selected ... e-mail ...URL ...", as broadly interpreted by the examiner.).

16. Further, as per claim 5 ***additionally reciting*** the limitation that; "The method in claim 2, wherein said storage means

is trusted and

has been previously verified using a

digital signature or

cryptographic checksum."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of recipient routing information, at the very least, via the user interface, the KERBEROS, the X.509 certificates data structures/authentication aspects per se, the certificate book, and Verisign third party authentication/certificate services aspects, clearly encompasses the "... trusted ... signature ... checksum ...", as broadly interpreted by the examiner.).

17. Further, as per claim 6 ***additionally reciting*** the limitation that; "The method in claim 2, wherein said digital signature provides verification with a trusted public key."
The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of recipient routing information, at the very least, via the user interface, the KERBEROS, the X.509 certificates data structures/authentication aspects per se, the certificate book, and Verisign third party authentication/certificate services aspects, clearly encompasses the "... signature ... verification ... key ...", as broadly interpreted by the examiner.).

18. Further, as per claim 7 ***additionally reciting*** the limitation that; "The method in claim 2, wherein said cryptographic checksum provides verification with a trusted key derived from

a Master Key,
a Session Key, or
a Message Key."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of recipient routing information, at the very least, via the user interface, the KERBEROS, the X.509 certificates data structures/authentication aspects per se, the certificate book, and Verisign third party authentication/certificate services aspects, clearly encompasses the "... checksum ... verification ... trusted ... session ... message ... key ...", as broadly interpreted by the examiner.).

19. Further, as per claim 8 ***additionally reciting*** the limitation that; "The method in claim 2, wherein the storage means is selected from the group consisting of

a Compact Certificate,

a chain of Compact Certificates leading to a trusted root public key, or

combinations thereof."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of recipient routing information, at the very least, via the user interface (i.e., inherently stored per se, both pre and post processing), the KERBEROS, the X.509 certificates data structures/authentication aspects per se, the certificate book, and Verisign third party authentication/certificate services aspects, clearly encompasses the "...Compact Certificate ... trusted root public key ...", as broadly interpreted by the examiner.).

20. Further, as per claim 10 ***additionally reciting*** the limitation that; "The method in claim 2, wherein the storage means is any conventional

e-mail message or

web page which the Sender trusts that has been copied into the Sender's messaging platform memory via mechanisms that the Sender trusts."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of recipient routing information for the email messaging, at the very least, via the user interface (i.e., inherently stored per se, both pre and post processing), the KERBEROS, the X.509 certificates data structures/authentication aspects per se, the certificate book, and Verisign third party authentication/certificate services aspects, clearly encompasses the "… e-mail … web page … trust …", as broadly interpreted by the examiner.).

21. Further, as per claim 11 ***additionally reciting*** the limitation that; "The method in claim 10, wherein the messaging platform is a messaging platform selected from the set consisting of:

a computer,

a server,

a PDA,

a telephone,

an appliance,

an information appliance,

a pager, or

any other device supporting such messaging."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of recipient routing information for the email messaging, at the very least, via the user interface, in itself at the very least, a computer; client and server configurations, (i.e., inherently stored per se, both pre and post processing), the KERBEROS, the X.509 certificates data structures/authentication aspects per se, the certificate book, and Verisign third party authentication/certificate services aspects, clearly encompasses the "… messaging … computer … any other device supporting such messaging …", as broadly interpreted by the examiner.).

22. Further, as per claim 12 ***additionally reciting*** the limitation that; "The method in claim 2, wherein

the OAEP padding seed and

the data encryption key are different values."

The teachings of Bellare, M., et al are directed towards such limitations of the use of RSA OAEP in order to "provide secrecy, ... message integrity ... (see, Bellare, M., et al, section 2.4, 7th full paragraph) in that the use of the RSA OAEP for the cryptographic functions would encompass the arbitrary use of seed values equal to, or not equal to the keying material.

23. Further, as per claim 13 ***additionally reciting*** the limitation that; "The method in claim 2, wherein

the OAEP padding seed and

the data encryption key are the same value to avoid the overhead of generating multiple random values."

The teachings of Bellare, M., et al are directed towards such limitations of the use of RSA OAEP in order to "provide secrecy, ... message integrity ... (see, Bellare, M., et al, section 2.4, 7th full paragraph) in that the use of the RSA OAEP for the cryptographic functions would encompass the arbitrary use of seed values equal to, or not equal to the keying material.

24. Further, as per claim 14 ***additionally reciting*** the limitation that; "The method in claim 2, wherein

the Sender's

private key and

certificate chain comprise fixed values shared among a plurality of

Senders."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of sender/recipient routing/configuration parameters information, at the very least, via the user interface; the KERBEROS, the X.509 certificates data structures/authentication aspects per se, the certificate book, and Verisign third party authentication/certificate services/root/chaining aspects, clearly encompasses the "... key ... certificate chain ... fixed values shared ...", as broadly interpreted by the examiner.).

25. Further, as per claim 15 ***additionally reciting*** the limitation that; "The method in claim 2, wherein

the Sender's

private key and

certificate chain fixed values are widely known."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of sender/recipient routing/configuration parameters information, at the very least, via the user interface; the KERBEROS, the X.509 certificates data structures/authentication aspects per se, the certificate book, and Verisign third party authentication/certificate services/root/chaining aspects, clearly encompasses the "... key ... certificate chain ... fixed values are widely known ...", as broadly interpreted by the examiner.).

26. Further, as per claim 16 ***additionally reciting*** the limitation that; "The method in claim 2, wherein

the Sender's

private key and

certificate chain fixed values are not widely known and

the Sender's software employs mechanisms to make it difficult to discover these values through a process of reverse engineering."

The teachings of Montville et al are directed towards such limitations (i.e., figures 1-14 and associated descriptions, whereas the setup of sender/recipient routing/configuration parameters information, at the very least, via the user interface; the KERBEROS, the X.509 certificates data structures/authentication aspects per se, the certificate book, and Verisign third party authentication/certificate services/root/chaining aspects, clearly encompasses the "... key ... certificate chain ... are not widely known ... difficult to discover ... reverse engineering", as broadly interpreted by the examiner.).

Allowable Subject Matter

Claims 9,21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

27. Claim 9 ***additionally reciting*** the limitation that; "The method in claim 2, wherein the storage means is a previously received Storymail story enabled message that was securely

received and

verified by mechanisms that are trusted for that kind of message."

28. Claim 21 ***additionally reciting*** the limitation that; "The method of claim 18, wherein said message is a Storymail story message."

Conclusion

29. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum
Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100